PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-161321
(43)Dat of publication of application : 18.06.1999

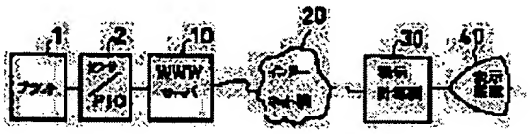
(51)Int.Cl. G05B 23/02
G06F 3/14
G06F 13/00
G06F 17/60

(21)Application number : 09-327981
(22)Date of filing : 28.11.1997

(71)Applicant : TOSHIBA CORP
(72)Inventor : INUBUSHI HIROYUKI

(54) PLANT MONITOR DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide the plant monitor device which transmits plant data from a remote plant by a desired computer and disables access from a person, a place, and a computer that are not allowed.
SOLUTION: This device has a data input part 2 which inputs data from a plant 1, a server 10 which inputs the data of the plant 1 from the data input part 2 and outputs them to the internet 20 or an intranet, and a computer 30 which is connected to the internet or intranet and inputs the data of the plant 1 sent from the sever 10, and the server 10 is equipped with a ciphering means which ciphers and outputs the plant data and outputs the data to a firewall for preventing illegal access from the internet 20.



LEGAL STATUS

[Date of request for examination] 27.01.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－161321

(43)公開日　平成11年(1999)６月18日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０５Ｂ	23/02		Ｇ０５Ｂ	23/02	Ｖ
Ｇ０６Ｆ	3/14	３２０	Ｇ０６Ｆ	3/14	３２０Ｃ
	13/00	３５５		13/00	３５５
	17/60			15/21	Ｚ

審査請求　未請求　請求項の数６　ＯＬ　（全５頁）

(21)出願番号　特願平9－327981

(22)出願日　平成９年(1997)11月28日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　犬伏　裕之
東京都府中市東芝町１番地　株式会社東芝府中工場内

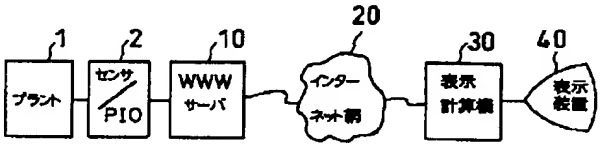
(74)代理人　弁理士　外川　英明

(54)【発明の名称】　プラント監視装置

(57)【要約】

【課　題】　遠隔のプラントからプラントデータを所望の計算機にて伝送し、利用を許可していない者、場所、計算機からのアクセスを出来ないようなプラント監視装置を提供する。

【解決手段】　プラントのデータを入力するデータ入力部と、このデータ入力部からプラントのデータを入力し、インターネット網あるいはイントラネット網に出力するサーバと、インターネット網あるいはイントラネット網に接続され、前記サーバから送信されるプラントのデータを取り込む計算機とを有し、サーバはプラントデータを暗号化して出力する暗号化手段を備えたり、インターネット網からの不正なアクセスを防止するファイヤウォールに出力する。



1

【特許請求の範囲】

【請求項１】　プラントのデータを入力するデータ入力部と、このデータ入力部からプラントのデータを入力し、インターネット網あるいはイントラネット網に出力するサーバと、インターネット網あるいはイントラネット網に接続され、前記サーバから送信されるプラントのデータを取り込む計算機とを有することを特徴とするプラント監視装置。

【請求項２】　請求項１のプラント監視装置において、前記サーバはプラントデータを暗号化して出力する暗号化手段を備え、前記計算機は送信されるデータを復号化する復号化手段を備えることを特徴とするプラント監視装置。

【請求項３】　プラントのデータを入力するデータ入力部と、前記データ入力部からプラントのデータを入力し、インターネット網からの不正なアクセスを防止するファイヤウォールに出力するサーバと、インターネット網に接続され、前記サーバから送信されるプラントのデータを前記ファイヤウォールを介して取り込む計算機とを有することを特徴とするプラント監視装置。

【請求項４】　プラントのデータを入力するデータ入力部と、前記データ入力部からプラントのデータを入力し、インターネット網からの不正なアクセスを防止する第一のファイヤウォールに出力するサーバと、インターネット網に接続される第二のファイヤウォールに接続され、前記サーバから送信されるプラントのデータを前記第二のファイヤウォールから取り込む計算機とを有することを特徴とするプラント監視装置。

【請求項５】　請求項３または請求項４のプラント監視装置において、前記ファイヤウォールは、ＶＰＮ機能を備えることを特徴とするプラント監視装置。

【請求項６】　請求項１，３または４のプラント監視装置において、前記計算機は、利用者を特定するセキュリティ機能を有し、当該セキュリティ機能の確認によりプラントのデータの取り込みあるいは表示を可能とするものであることを特徴とするプラント監視装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はインターネット網あるいはイントラネット網を用いたプラント監視装置に関する。

【０００２】

【従来の技術】工業プラント、発電プラント、電力系統等のプラントでは、図９のように、ある程度距離が離れると、伝送装置を用いて、プラントのデータを伝達している。図中センサ／ＰＩＯは、一つの形態であってプラント監視の対象がディジタル化されている場合は、単にデータ入力装置となる場合もある。

【０００３】また、遠隔地からの監視をする場合には、従来では、専用回線を用いたりＩＳＤＮを利用するのが一般的であった。発電プラント等でも、発電所と本店間の監視には、専用回線を使用している。この専用回線やＩＳＤＮの利用では、コスト高となる問題がある。

2

【０００４】しかし、従来はインターネットの技術がなかったことまた、インターネット自体は、ビジネス向けに、比較的静的な情報（変化がゆっくりとしたもの）を表示していることから、プラント情報のようにたえず変化する動的な情報を伝送表示するという発想がなかった。

【０００５】また、、表示しようとしても、例えば発電所のようなデータをインターネットを用いて表示するには、以下の様な問題がありその実現は難しかった。

（１）インターネットは、データが網の目の様にはりめぐらされたネットワークを、途中にあるサーバを経由しながら伝送されていくため、途中のサーバで、そのデータを盗聴しようと考えれば、可能である。

（２）インターネットは、世界中に広がるネットワークであるので、ＵＲＬと呼ばれるインターネットのWWWサーバのアドレスが知られてアクセスされると、第三者に容易に中味を見られてしまう。

（３）仮にある端末（表示装置）のみから見られるようにしていても、その端末に近づくことができれば、利用を許可していない人でも、電源を入れて表示装置から情報を見ることも可能であった。

【０００６】このように、利用を許可していない人間からデータを守るために、セキュリティを強化する必要があったが、これに必要な技術をうまく組み合わせて利用することができなかった。

【０００７】

【発明が解決しようとする課題】そこで、本発明では、利用を許可していない人、場所からは、容易にデータを見ることができない様な、プラント監視装置を提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明のプラント監視装置は、プラントのデータを入力するデータ入力部と、このデータ入力部からプラントのデータを入力し、インターネット網あるいは、イントラネット網に出力するサーバと、インターネット網あるいはイントラネット網に接続され、前記サーバから送信されるプラントのデータを取り込む計算機とを有する。

【０００９】そして、このプラント監視装置のサーバはプラントデータを暗号化して出力する暗号化手段を備え、計算機は送信されるデータを復号化する復号化手段を備える。

【００１０】また、本発明のプラント監視装置は、プラントのデータを入力するデータ入力部と、前記データ入力部からプラントのデータを入力し、インターネット網からの不正なアクセスを防止するファイヤウォールに出力するサーバと、インターネット網に接続され、前記サ

ーバから送信されるプラントのデータを前記ファイヤウォールを介して取り込む計算機とを有する。

【００１１】また、プラントのデータを入力するデータ入力部と、前記データ入力部からプラントのデータを入力し、インターネット網からの不正なアクセスを防止する第一のファイヤウォールに出力するサーバと、インターネット網に接続される第二のファイヤウォールに接続され、前記サーバから送信されるプラントのデータを前記第二のファイヤウォールから取り込む計算機とを有する。

【００１２】そして、このファイヤウォールは、ＶＰＮ機能を備える。また、本発明のプラント監視装置において、前記計算機は、利用者を特定するセキュリティ機能を有し、当該セキュリティ機能の確認によりプラントのデータの取り込みあるいは表示を可能とするものである。

【００１３】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照して説明する。図１は、本発明の最も基本的な技術的思想を示すものである。第１実施の形態の図１は、従来の図９の専用回線１２０の代りに、インターネット網２０を用いている点が大きく異なる。また、図９では、専用回線１２０の両端は伝送装置１１０と１３０であるのに対して、図１ではWWWサーバ１０と表示計算機３０である。WWWサーバ１０は、インターネットを実現するデータをもっているところである。一方、表示計算機３０は一般にパソコンで実施している。

【００１４】データ入力部のセンサ／ＰＩＯ２は、プラント１からのデータを入力する。WWWサーバ１０は、前記センサ／ＰＩＯ２が入力したデータを、入力処理し、インターネットで利用できるデータ形式に処理を行い、インターネット網２０に出力する。

【００１５】表示計算機３０では、このデータを入力して、プラント状態を表示装置４０に表示する。次に、第２の実施の形態を図２について説明する。

【００１６】第１実施形態の場合は、インターネット網を使うため、セキュリティの問題がある。そこで、インターネット網の代りに、イントラネット網を用いる。インターネットが公衆の網であるのに対して、イントラネットは、企業内の専用の網である。従って、専用回線を用いたのと同じになるため、社外のメンバからの不正アクセスは阻止できる。

【００１７】次に、第３の実施の形態を図３について説明する。網は、インターネット網を使うが、ファイヤウォールという情報の防火壁を設けることにより、不正なアクセスを防止することができる。

【００１８】次に、第４の実施の形態を図４について説明する。基本的には図１と同じであるが、WWWサーバと、表示計算機に暗号化プロトコルが組み込まれている点が異なる。「暗号化プロトコルとは、ＯＳＩ参照でいう、物理層，ネットワーク層，セクション層，アプリケーション層で主に用いられているプロトコルで、その代表的なものがＳＳＬである。」ＳＳＬ（Secure Sockets Layer）は、サーバと、WWWブラウザのためにセキュリティ機構として、Ｗ３Ｃワーキンググループのセキュリティ部門によって提案された通信方式である。これは、通信において特定のある部分だけを暗号化するのではなく、インターネットの基本的なプロトコルであるＴＣＰ／ＩＰで通信される内容の全てを暗号化するものである。ＳＳＬの場合、通常WWWブラウザに組み込まれるため、使用者は意識する必要がない。

【００１９】また、WWWサーバと表示計算機時間のデータが全て暗号化されているので仮に、この間で流れているデータが盗まれても、盗んだ人は解読できないので、実用上、問題ない。現在、ＳＳＬに類似のものでは、ＰＣＴ（Private Comunication Technology）等がある。

【００２０】次に、第５の実施の形態の図５について説明する。図３のファイヤウォールにさらに、ＶＰＮ（バーチャルプライベートネットワーク）の機能をもたせたものである。ＶＰＮも、前述のＳＳＬと同様に暗号化する機能があり、さらに、トンネリング機能という機能も同時に実現する。このトンネリング機能とは、予め決められたトンネル（経路）でしか、インターネットがアクセスできないようにする機能である。

【００２１】つまり、“経路”は、ＩＰアドレスという固有の接続点で識別され、当該のＩＰアドレスをもった利用者からしかアクセスできないようになる。これにより、従来の問題点の“許可している場所”以外からのアクセスはシャットアウトすることができる。

【００２２】一般に、ＶＰＮの機能はファイヤウォールにもたせている。この実施例では、暗号化されたデータを復号化するために表示計算機側にもＶＰＮ機能付きのファイヤウォールを設けている。

【００２３】次に、第６の実施の形態の図６について説明する。第５実施によると、特定の端末からでないと利用できないとしても、その端末に近づくことができる人であれば、電源を入れて表示装置を生かし、表示端末からデータが自由にひき出せてしまう。そこで、表示計算機にＩＣカード読みとり機をつけて、予め登録してあるＩＣカードを使用する人からしか、表示計算機がさわれないようにするものである。ここでは、ＩＣカードとしているが、これに類する磁気カード等でも同様に扱えることは言うまでもない。

【００２４】次に、第７の実施の形態を図７について説明する。図６では、操作する人が妥当か否かをＩＣカードという本人が所持しているものを用いて判定した。

【００２５】一方、図７では、ＩＣカードの代りに、操作する人のバイオメトリクス（生体情報）を用いる。バイオメトリクスとは、個人の身体的特徴（指紋や掌紋

5

等）や、個人の行為（筆跡，声紋）を用いて、本人であるかを識別することをさす。考え方は、図６と同様である。予め本人データを登録しておき、このデータと、バイオメトリクスセンサ経由で入力されたデータが一致したら、表示用計算機のアクセスを許可する。バイオメトリクスのために指紋を用いれば、バイオメトリクスセンサは“指紋読みとり器”となる。

【００２６】次に、第８の実施の図８について説明する。これは、図６とほぼ同様であるが、ＩＣカードの代りに、本人のＩＤ番号と、このＩＤ番号に対応するパスワードを使うものである。アクセスを開始する際に、操作する人は、ＩＤ番号とパスワードを入れなければ、中味を見ることができない。ごく簡単なやり方としては、この図８の装置で実現できるが、インターネット網を流れるデータは、暗号化されていないので、クラッカー（ハッカー）と呼ばれる悪意をもった人からは、簡単にＩＤ番号と、パスワードが盗まれるという欠点はある。

【００２７】従って、実際には図８は、暗号化技術を使用する図４，図５の装置方法と組合せて実現することになる。尚、ＩＤ番号は、１人ずつ違うものを割りあてておく。またアクセス記録は定期的にチェックし、本人からのアクセスであるかをチェックすることができる。

【００２８】以上のように、発明によれば、従来専用の通信回線を、設けなければ実現できなかったものが、インターネット網により簡単に遠隔の監視を行うことができ、通信回線が不要となる。その結果、大幅なコストの削減も可能になる。具体的なコストは、距離等によるので、一概には言えないが、専用回線を確立するには、１００万円～１０００万円オーダ以上の費用がかかる。これに対し、インターネット網が利用できればこのコストの１／１０～１／１００以下のコストで通信が可能と考えられる。また、計算機の設置場所の変更、増設についても対応が容易にできる。

【００２９】また、不正アクセス者が、WWWサーバのＵＲＬを知れば簡単に見られる危険があったものが、ファイヤウォールにより、予め登録されたアクセス者またはアクセス装置からの接続しか許可しないため、より安全に通信を行うことが可能となる。

【００３０】また、通信網上のデータが暗号化されていないので、クラッカー等からデータ自体の盗聴をされると、そのまま内容が流出してしまうことになっていたものが、暗号化により見られても内容までは解読できないことにより、セキュリティを確保することが可能となる。

【００３１】また、本発明によれば、ＶＰＮの機能により、データが暗号化されるとともに、トンネリングの機能により“許可している場所（ＩＰアドレス）”以外からのアクセスをシャットアウトすることが可能となる。

【００３２】また、本発明によれば、ＩＣカードを所持した人間からしかアクセスが許可されないので、不正なアクセスを防止することができる。例えば、請求項５を適用しても、電源を入れてその端末からアクセスされてしまう可能性があったが、このＩＣカードを用いれば、当該のＩＣカードを所持している請求項７の発明によれば、バイオメトリクス（指紋等）が一致した人間からしかアクセスが許可されないので、不正なアクセスを防止することができる。

【００３３】また、本発明によれば、ＩＤ番号とパスワードを知っている人からしかアクセスできないので、不正なアクセスを防止することができる。また、何らかの方法で不正アクセス者が、ＩＤ番号とパスワードを盗んでしまっても、少くともアクセス記録は残るので、これをもとに不正アクセス者を割り出すことができる等の効果も期待できる。

【００３４】

【発明の効果】本発明によれば、遠隔のプラントのデータを簡単かつ安全に送信できるプラント監視装置を提供できる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態のプラント監視装置の構成図

【図２】本発明の第２の実施形態のプラント監視装置の構成図

【図３】本発明の第３の実施形態のプラント監視装置の構成図

【図４】本発明の第４の実施形態のプラント監視装置の構成図

【図５】本発明の第５の実施形態のプラント監視装置の構成図

【図６】本発明の第６の実施形態のプラント監視装置の構成図

【図７】本発明の第７の実施形態のプラント監視装置の構成図

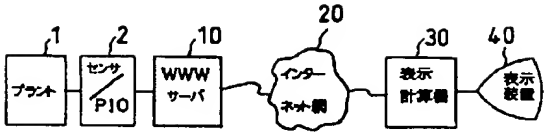
【図８】本発明の第８の実施形態のプラント監視装置の構成図

【図９】従来のプラント監視装置の構成図である。

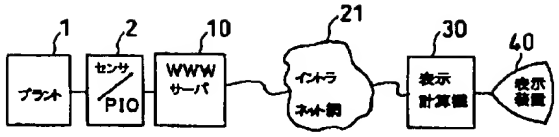
【符号の説明】

１…プラント、２…データ入力部（センサ／ＰＩＯ）、１０、１３…WWWサーバ、１１，１２，３２…ファイヤウォール、２０…インターネット網、２１…イントラネット網、３０，３１…計算機、４０…表示装置

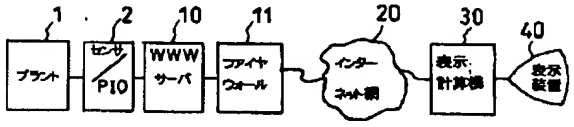
【図１】



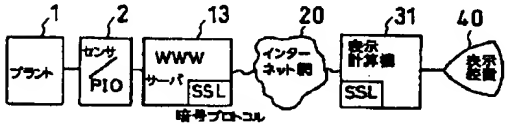
【図２】



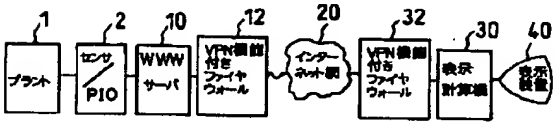
【図３】



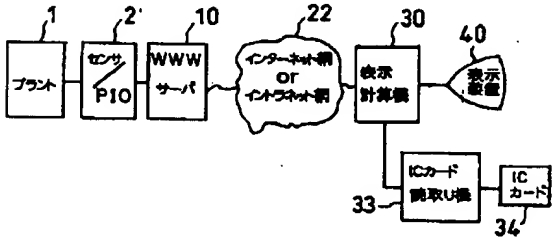
【図４】



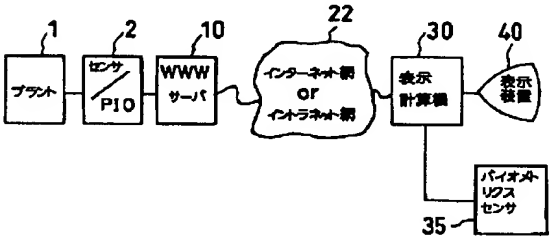
【図５】



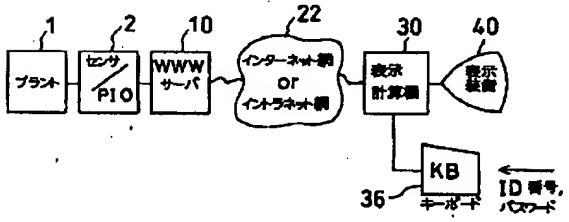
【図６】



【図７】



【図８】



【図９】